FireEye

The Pyramid of Pain

Intel-Driven Detection & Response to Increase Your Adversary's Cost of Operations

The Wacky Wall Walker Approach

The most common approach to "threat intel" I see is…

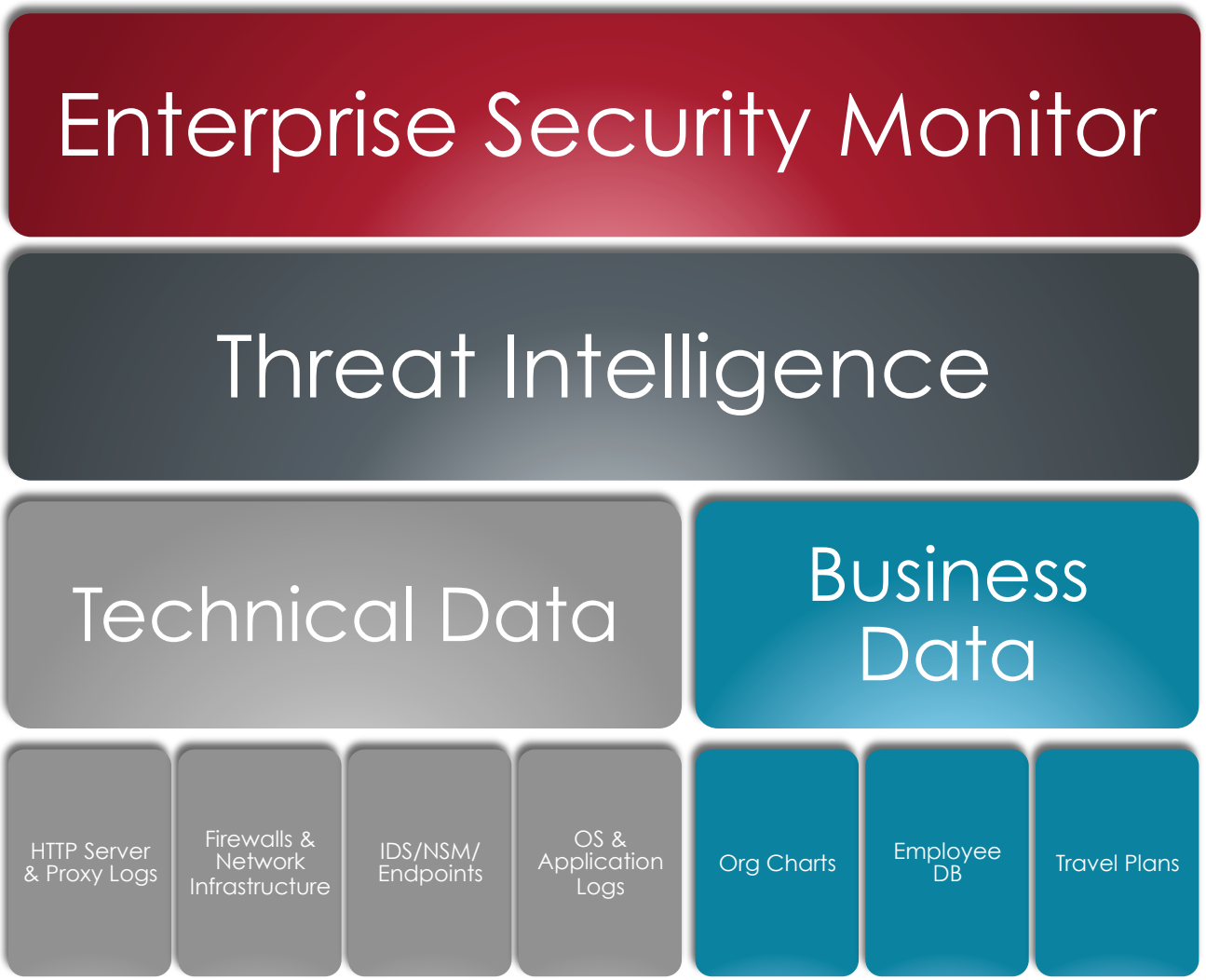
THROW ALL OUR FACTS OUT THERE AND SEE WHAT STICKS.

Pros	Cons
Quick to implement	Too many alerts No confidence in results Gives your adversaries a laugh

We can do better!

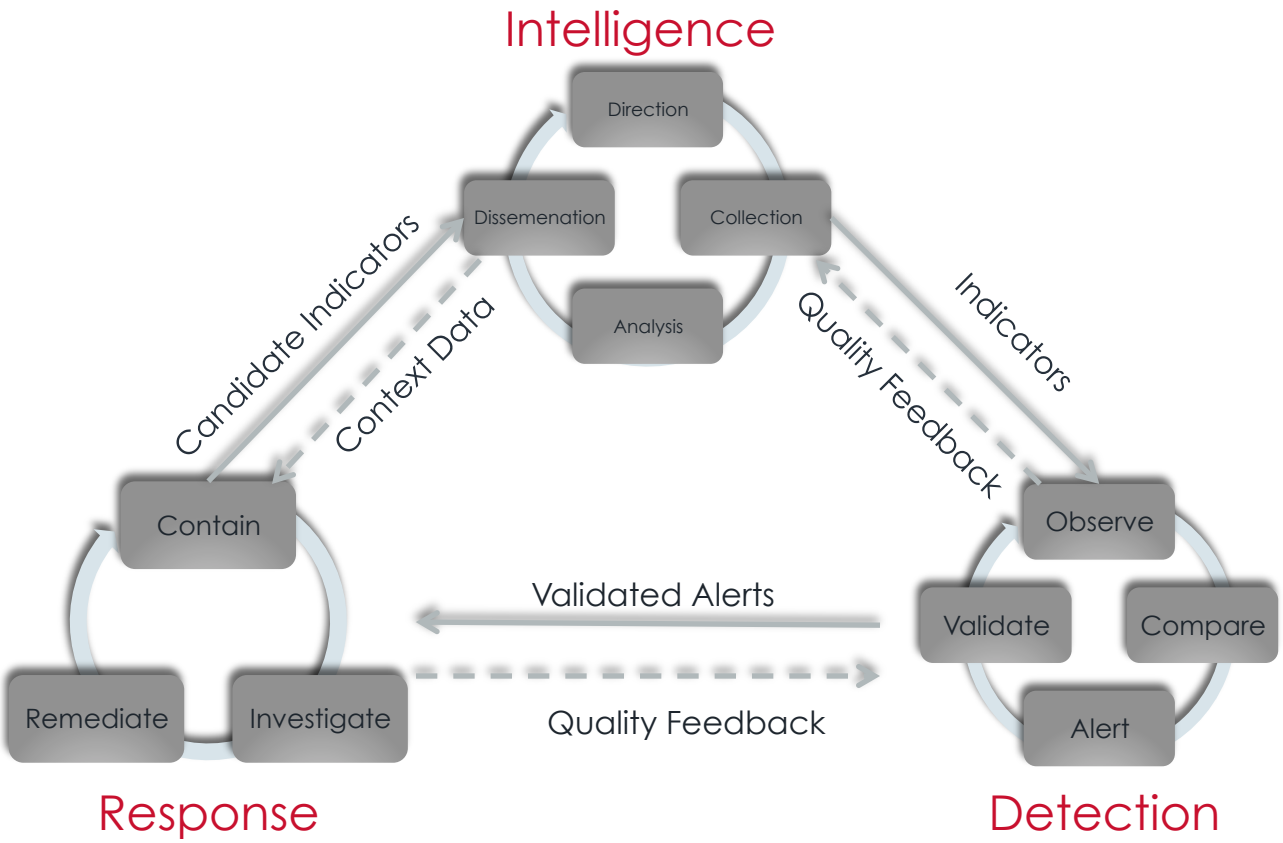
FireEye

Enterprise Security Monitoring



FireEye

The Intel-Driven Operations Cycle



FireEye

Let's be clear…

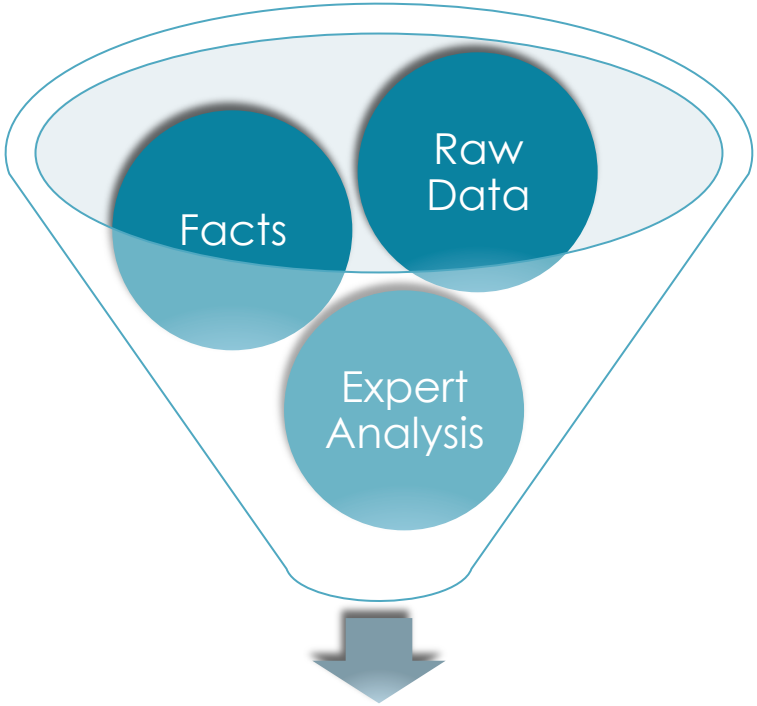
Most people confuse  with intelligence.

Let's Be Clear…

Captain, I do not believe that to be the correct use of the term.

Let's Be Clear…

The Reality is More Complicated



Intelligence!

FireEye

Indicators, the Avatars of Intelligence

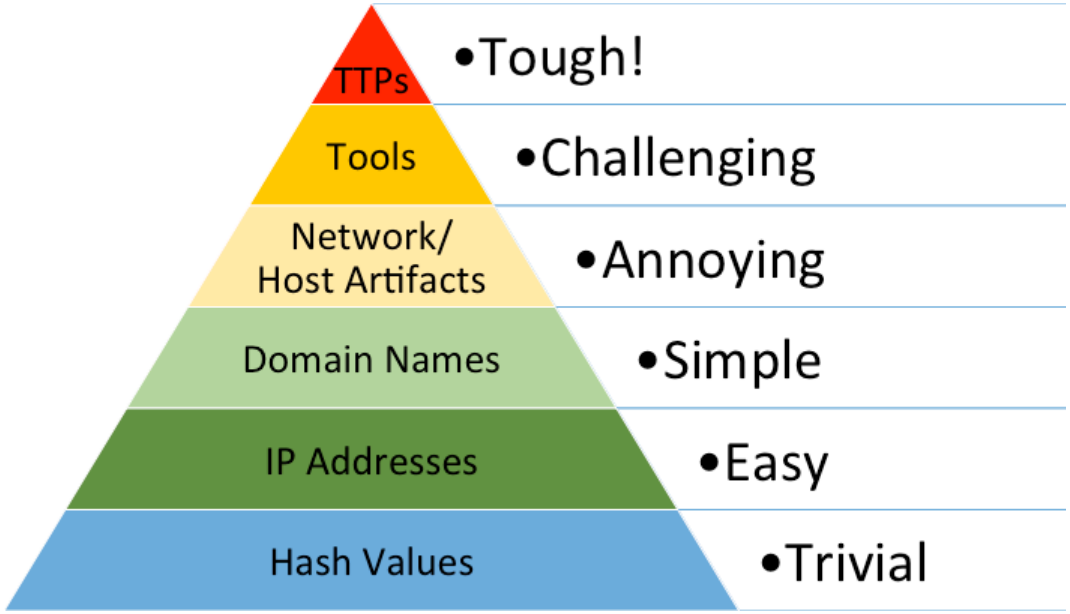
A piece of information that points to a certain conclusion

What it is not

≠

FireEye

The Pyramid of Pain



The Pyramid measures **potential usefulness** of your intel

It also measures **difficulty of obtaining** that intel

The higher you are, the **more resources** your adversaries have to expend.

When you quickly detect, respond to and disrupt your adversaries' activities, defense becomes offense.

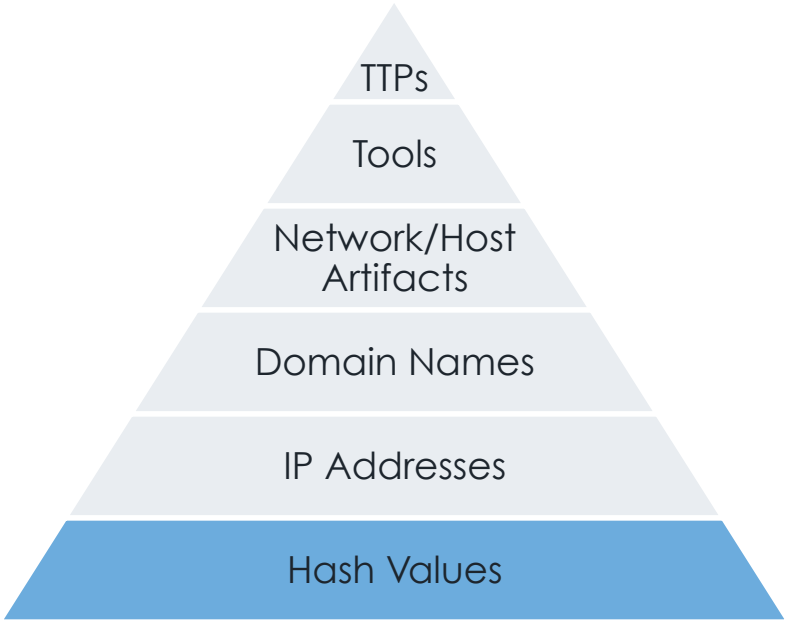
FireEye

Hashes

Hashes are, by far, the highest confidence indicators.

Unfortunately, they are extremely susceptible to change (even accidentally).

Hashes are probably the least useful type of indicators.



MD5
5f6ce162c4b5516670d5a8f1f8f4e57b
SHA1
C8d4c389beaff88811f8fab1965519fce74ffd8a
SHA256
ad690662a1faf97dc41387b73f8fd3415d64f9b0ce66db3e9134385d94e0c01b

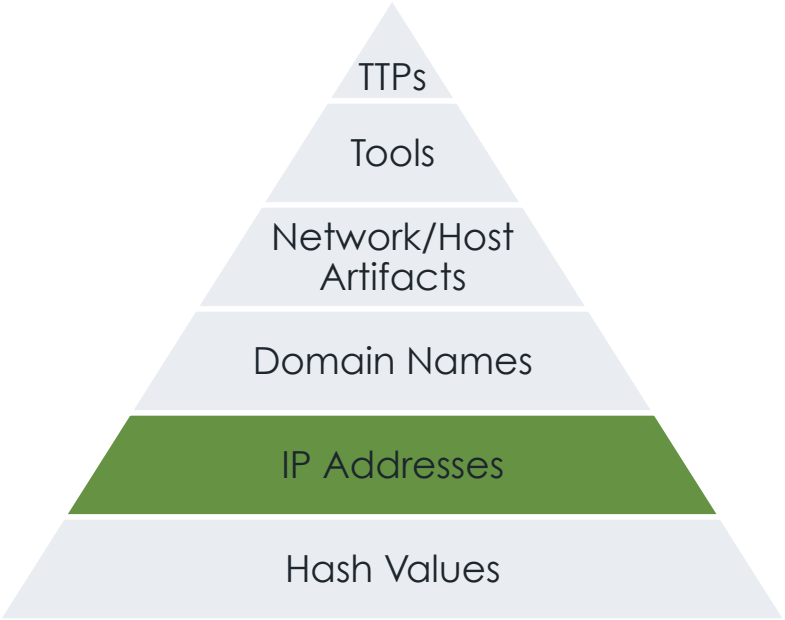
FireEye

IP Addresses

Only `n00bs` use their own addresses.

VPNs, Tor, open proxies all make it trivial to change your IP.

If it's hardcoded into a config, maybe adversaries have to do a little work to update it.



Dotted Decimal 192.168.1.1 **Dotted Hex** 0xC0.0xA8.0x01.0x01 **Dotted Octal** 0300.0250.0001.0001	**Decimal** 3232235777 **Hex** 0xC0A80101 **Octal** 030052000401

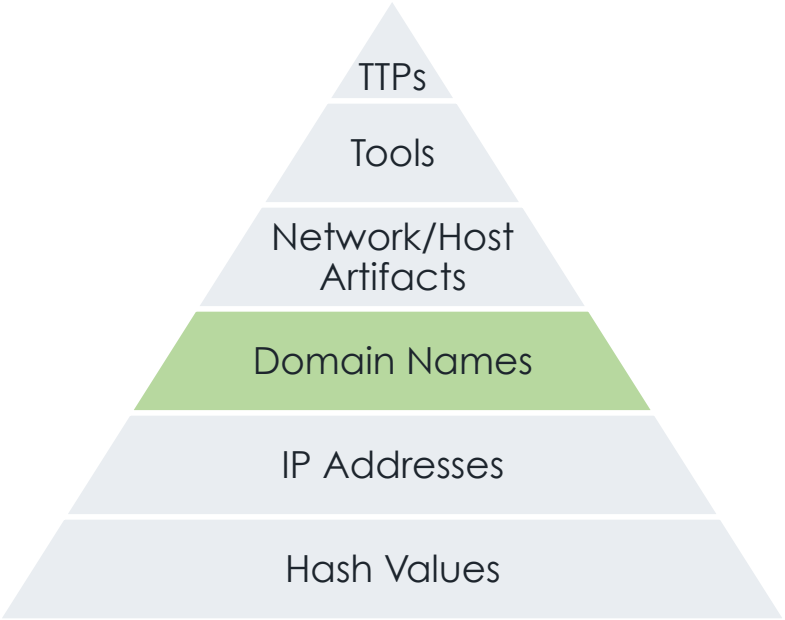
FireEye

Domain Names

Almost as easy to change as IP addresses.

Domains require pre-registration and (usually) a fee, but there are ways around this.

Dynamic DNS providers even help automate the adversary's update process with helpful APIs.



Unicode 邪悪なドメイン.com **Punycode** Xn—q9j5f9d1dzdq306auhtd.com	**Legitimate Domain** rvasec.com **Malicious Homograph** rvasec.com

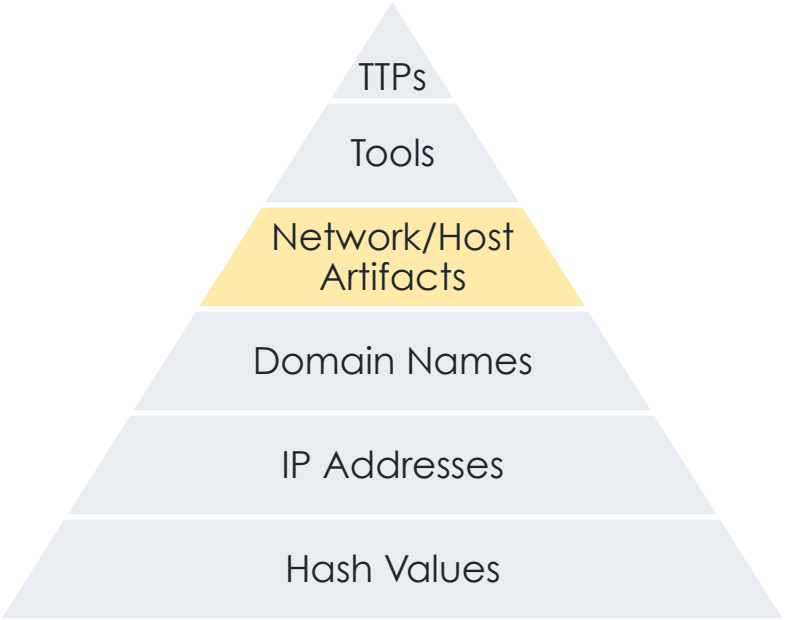
FireEye

Network & Host Artifacts

It's very difficult to perform useful activities without leaving some traces.

On hosts, look for files & directories, registry objects, mutexes, memory strings […]

On the network, check for distinctive transaction values, especially protocol errors or just misinterpretations.



Distinctive URI patterns
/^[A-F0-9]{16}\/\d{3,5}\.{php|aspx}$/
User-Agent Strings
xi/1.0
Typos
Mozilla/5.0 (compatible; MSIE7.0; Windows NT 6.1;)

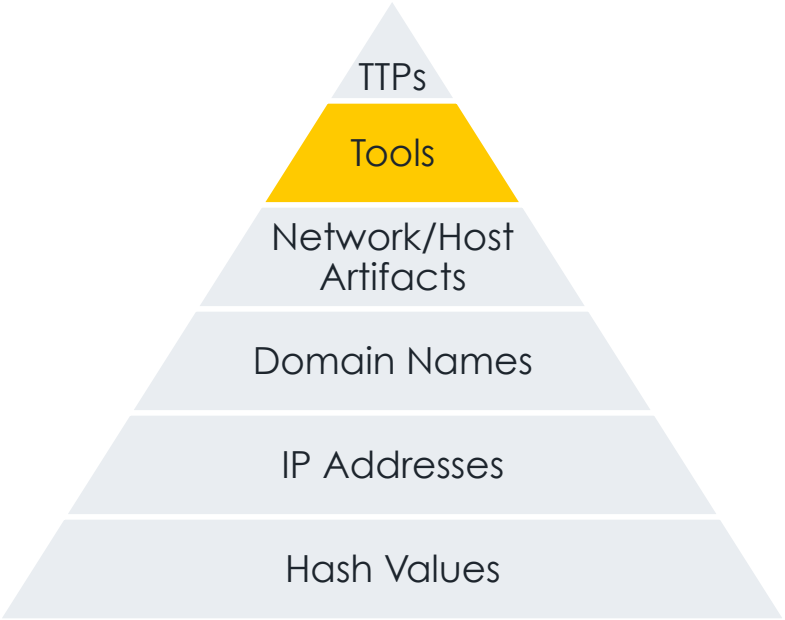
FireEye

Tools

If you see the same tool over and over, you eventually get really good at detecting it.

No matter what incidental changes they make, your detection mechanisms can deal with them.

To continue, they need a new tool. With testing & training time, that's a real victory!



Once upon a time, there was an incident response team who encountered the same tool over and over again for more than a year. The tool had a bolt-on network front end, so the attackers could easily change the network protocol, but the back end was always the same. Eventually, the IR team realized that the distinctive keep-alive function was part of the back end, and could be reliably detected. And then everyone (except the attacker) slept well at night and lived happily ever after!

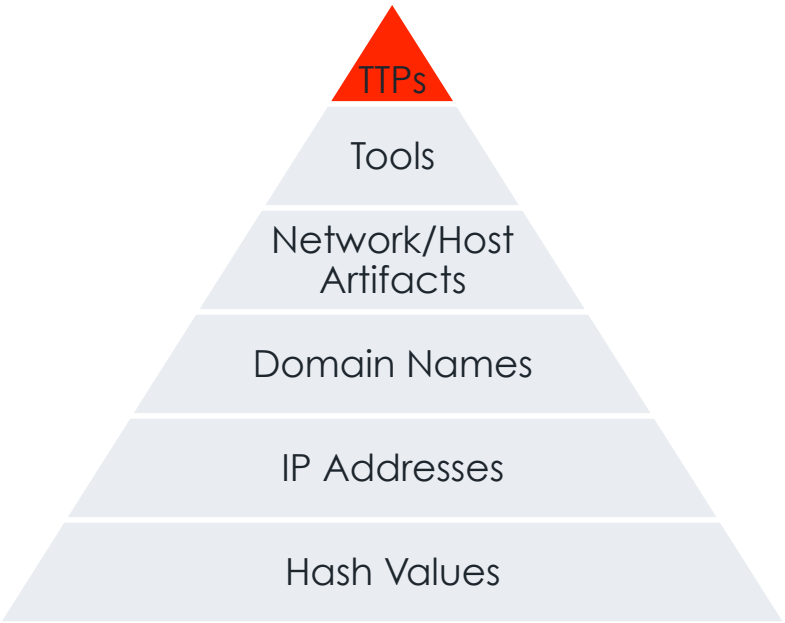
FireEye

Tactics, Techniques & Procedures

TTPs are the expression of the attacker's training.

Retraining is probably the hardest thing you can do once, let alone continually.

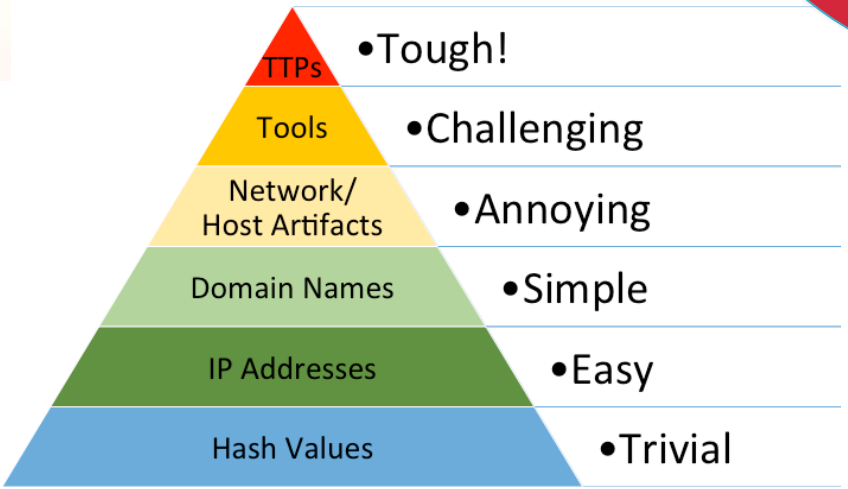
This becomes so expensive that they have to question their commitment to attacking you. Win!



Data Staging Tactic
Create encrypted RAR and transfer them to the exfiltration point.
Data Staging Technique
AES encryption, files of exactly 650,000 bytes, file copies via SMB
Data Staging Procedure
winrar a –hpqwerty –r vacation_photos.rar *staging_dir*
net use *exfil_server*\photos

FireEye

In Summary



FireEye

Questions?

David J. Bianco

David.Bianco@mandiant.com

@DavidJBianco

detect-respond.blogspot.com

FireEye